UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,800	12/01/2000	Niels Mache	450117-02961	5593

20999 7590 08/26/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/728,800	MACHE, NIELS	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-15 and 18-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-15 and 18-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the Request for Continued Examination (RCE) filed on June 9, 2005. Claims 1-21 were originally received for consideration. Per the After-Final amendment received on April 1, 2005, claims 1,5,10,11, and 15 have been amended, and claims 6-7, and 16-17 have been cancelled by virtue of the amendment received July 23, 2004. Claims 1-5, 8-15, and 18-21 are currently being considered.

Response to Arguments

2. Applicant's arguments, see page 10, filed April 1, 2005, with respect to the rejection(s)of claim(s) 1,5,11, and 15 under Misra et al. (U.S. Patent No. 5,757,920) have been fully considered and are persuasive. The applicant argues that "the supposition that the ticket includes a time stamp does not inherently show that the client verifies the ticket" (page 10, lines 9-10). Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Misra et al. (U.S. Patent No. 7,757,920) in view of Haber et al. (U.S. Patent No. 5,781,629).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 1 – 5, 8 – 15, 18 – 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra et al. (U.S. Patent 5,757,920) in view of Haber et al. (U.S. Patent No. 5,781,629).

Regarding claim 1, Misra discloses:

Method for the authentication of data communicated from a originator to a destination, wherein a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data (Figure 2A, column 5 line 47 – column 6 line 31).

Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a previously stored temporal validity information. Misra discloses a logon certificate which contains a time stamp and temporal information which insure that the certificate containing the session key is valid (Figure 2A, column 46 – 55). This logon certificate is used to log onto a domain. Once logged into the domain/system, the

server verifies the authenticity of the key and sends a new session key (acknowledgment key) to the client along with a ticket (column 8 lines 37 – 65). Misra disclose that the session key and ticket (acknowledgement key) can contain authorization data including a data structure similar to an authenticator which includes a time stamp (column 7 lines 35 – 52). Misra does not explicitly mention that the client uses the time stamp to verify the ticket. Haber discloses a digital document authentication system, which uses a time stamped certificate to authenticate the document that it is sent with (column 1 line 66-column 2 line 4). The document is analogous to the session key of Misra and the time stamped certificate is equated to the ticket of Misra, as Haber notes that the document is "any sequence of bits" (column 1 lines 61-62). The time stamp of Haber is checked to validate that the given document was created by the correct party at the time noted on the time stamp certificate. If the document (session key) and the time stamp certificate (ticket) do not correlate, then the authentication test fails, and it is known that the document (session key) is not valid. Therefore, using the time stamp on the ticket, allows the client to verify the authenticity and the validity period of the session key, which according to Haber, satisfies the "need to establish the date and time at which a document was created and to prove that the document in question has not been modified since then" (column 1 lines 14-18). Furthermore, Misra states that the time stamp "helps to minimize the time period in which an eavesdropper may used a copied ticket and authenticator pair" (column 45 – 52). Therefore, it would have been obvious to add a time stamp to the acknowledgement key received at the originator from the destination to help minimize

the time period that an eavesdropper may use a intercepted session key and to establish the date and time at which the session key was created and to prove that the session key has not been modified by a third party.

Regarding claim 5, Misra discloses:

Method for the authenticated transmission of messages, comprising the following communication setup steps:

generating a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key (column 5 line 47 – column 6 line 31);

transmitting the login key from an originator to a destination (column 7 lines 10-21); and

verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side (column 8 lines 45 – 65); and comprising the following acknowledgement steps:

in case the verification of the authenticity and the temporal validity of the login key is positive,

generating an acknowledgement key by a keyed-hashing method on the basis of second random data and the private key (column 8 lines 45 – 65);

transmitting the acknowledgement key from the destination to the originator (Figure 4B, column 8 lines 60-65); and

verifying the acknowledgement key by the originator, including checking the acknowledgment key (column 8 line 66 – column 9 line 9).

furthermore comprising the following acknowledgement steps:

Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a previously stored temporal validity information. Misra discloses a logon certificate which contains a time stamp and temporal information which insure that the certificate containing the session key is valid (Figure 2A, column 46 – 55). This logon certificate is used to log onto a domain. Once logged into the domain/system, the server verifies the authenticity of the key and sends a new session key (acknowledgment key) to the client along with a ticket (column 8 lines 37 – 65). Misra disclose that the session key and ticket (acknowledgement key) can contain authorization data including a data structure similar to an authenticator which includes a time stamp (column 7 lines 35 – 52). Misra does not explicitly mention that the client uses the time stamp to verify the ticket. Haber discloses a digital document authentication system, which uses a time stamped certificate to authenticate the document that it is sent with (column 1 line 66-column 2 line 4). The document is analogous to the session key of Misra and the time stamped certificate is equated to the ticket of Misra, as Haber notes that the document is "any sequence of bits" (column 1 lines 61-62). The time stamp of Haber is checked to validate that the given document was created by the correct party at the time noted on the time stamp certificate. If the document (session key) and the time stamp certificate (ticket) do not correlate, then the authentication test fails, and it is known that the document (session key) is not valid. Therefore, using the time stamp on the ticket, allows the client to verify the authenticity and the validity period of the session key,

which according to Haber, satisfies the "need to establish the date and time at which a document was created and to prove that the document in question has not been modified since then" (column 1 lines 14-18). Furthermore, Misra states that the time stamp "helps to minimize the time period in which an eavesdropper may used a copied ticket and authenticator pair" (column 45 – 52). Therefore, it would have been obvious to add a time stamp to the acknowledgement key received at the originator from the destination to help minimize the time period that an eavesdropper may use a intercepted session key and to establish the date and time at which the session key was created and to prove that the session key has not been modified by a third party.

Regarding claim 11, Misra discloses:

Distributed system for communicating authenticated data from a originator to a destination, designed for a keyed hashing technique according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data (Figure 2A, column 5 line 47 – column 6 line 31).

Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a previously stored temporal validity information. Misra discloses a logon certificate

which contains a time stamp and temporal information which insure that the certificate containing the session key is valid (Figure 2A, column 46 – 55). This logon certificate is used to log onto a domain. Once logged into the domain/system, the server verifies the authenticity of the key and sends a new session key (acknowledgment key) to the client along with a ticket (column 8 lines 37 – 65). Misra disclose that the session key and ticket (acknowledgement key) can contain authorization data including a data structure similar to an authenticator which includes a time stamp (column 7 lines 35 – 52). Misra does not explicitly mention that the client uses the time stamp to verify the ticket. Haber discloses a digital document authentication system, which uses a time stamped certificate to authenticate the document that it is sent with (column 1 line 66-column 2 line 4). The document is analogous to the session key of Misra and the time stamped certificate is equated to the ticket of Misra, as Haber notes that the document is "any sequence of bits" (column 1 lines 61-62). The time stamp of Haber is checked to validate that the given document was created by the correct party at the time noted on the time stamp certificate. If the document (session key) and the time stamp certificate (ticket) do not correlate, then the authentication test fails, and it is known that the document (session key) is not valid. Therefore, using the time stamp on the ticket, allows the client to verify the authenticity and the validity period of the session key, which according to Haber, satisfies the "need to establish the date and time at which a document was created and to prove that the document in question has not been modified since then" (column 1 lines 14-18). Furthermore, Misra states that the time stamp "helps to minimize the time period in which an eavesdropper may used a copied

ticket and authenticator pair" (column 45 – 52). Therefore, it would have been obvious to add a time stamp to the acknowledgement key received at the originator from the destination to help minimize the time period that an eavesdropper may use a intercepted session key and to establish the date and time at which the session key was created and to prove that the session key has not been modified by a third party.

Regarding claim 15, Misra discloses:

Distributes system for the authenticated transmission of messages, comprising:
an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key (column 5 line 47 – column 6 line 31);
a network for transmitting the login key from the originator to a destination (column 7 lines 10-21),
wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest (column 8 lines 45 – 65).

Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a previously stored temporal validity information. Misra discloses a logon certificate which contains a time stamp and temporal information which insure that the certificate containing the session key is valid (Figure 2A, column 46 – 55). This logon certificate is used to log onto a domain. Once logged into the domain/system, the server verifies the authenticity of the key and sends a new session key (acknowledgment key) to the client

along with a ticket (column 8 lines 37 – 65). Misra disclose that the session key and ticket (acknowledgement key) can contain authorization data including a data structure similar to an authenticator which includes a time stamp (column 7 lines 35 – 52). Misra does not explicitly mention that the client uses the time stamp to verify the ticket. Haber discloses a digital document authentication system, which uses a time stamped certificate to authenticate the document that it is sent with (column 1 line 66-column 2 line 4). The document is analogous to the session key of Misra and the time stamped certificate is equated to the ticket of Misra, as Haber notes that the document is "any sequence of bits" (column 1 lines 61-62). The time stamp of Haber is checked to validate that the given document was created by the correct party at the time noted on the time stamp certificate. If the document (session key) and the time stamp certificate (ticket) do not correlate, then the authentication test fails, and it is known that the document (session key) is not valid. Therefore, using the time stamp on the ticket, allows the client to verify the authenticity and the validity period of the session key, which according to Haber, satisfies the "need to establish the date and time at which a document was created and to prove that the document in question has not been modified since then" (column 1 lines 14-18). Furthermore, Misra states that the time stamp "helps to minimize the time period in which an eavesdropper may used a copied ticket and authenticator pair" (column 45 – 52). Therefore, it would have been obvious to add a time stamp to the acknowledgement key received at the originator from the destination to help minimize the time period that an eavesdropper may use a

intercepted session key and to establish the date and time at which the session key was created and to prove that the session key has not been modified by a third party.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to claim 1, characterized in that the temporal validity information can be defined by the originator (column 5 line 47-55).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to anyone of the preceding claims, characterized in that the data comprises random data which are unique for a time span defined by the temporal validity information (column 5 line 47-55).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to anyone of the preceding claims, characterized in that the data is a login key for a communication setup (column 5 lines 47-55).

Misra describes a session key (Figure 2A item 120), which is analogous to the login key delineated in above claim 4.

Claim 8 is rejected as applied above in rejecting claim 5. Furthermore, Misra discloses:

Method according to claim 5, furthermore comprising the following message transmission steps: in case the verification of the acknowledgment key is positive,

extracting the second random data from the acknowledgment key, generating a message by a keyed-hashing method on the basis of the second random data, message data and the private key, transmitting the message from the originator to the destination, and, verifying the message by the destination (column 8 line 66 – column 9 line 9).

Claim 10 is rejected as applied above in rejecting claim 5. Furthermore, Misra discloses:

A storage medium storing a software program product, characterized in that the software program product implements, when loaded into a computing device of a distributed system, a method according to claim 5 (column 5 line 47 – column 6 line 31, column 7 lines 10-21, column 8 lines 45 – 65).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the originator is designed to define the temporal validity information (column 5 line 47-55).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the data comprises random data which are unique for a time span defined by the temporal validity information (column 5 line 47-55).

Claim 14 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the data is a login key for a communication setup (column 5 lines 47-55).

Misra describes a session key (Figure 2A item 120), which is analogous to the login key delineated in above claim 4.

Claim 18 is rejected as applied above in rejecting claim 15. Furthermore, Misra discloses:

Distributed system according to claim 15, characterized in that the originator is designed to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and the destination is designed to verify the message (column 8 line 66 – column 9 line 9).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Misra discloses:

Method according to claim 8, characterized in that the message furthermore comprises a time stamp of the message and when verifying the message it is checked on the basis of the time stamp and the temporal validity information whether the message is still valid (column 5 line 47 – column 6 line 31).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Misra discloses:

Distributed system according to claim 18, characterized in that the message furthermore comprises a time stamp and when verifying the message, the destination checks on the basis of the time stamp of the message and the temporal validity information whether the message is still valid (column 5 line 47 – column 6 line 31).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to claim 1, characterized in that the data is a message (column 5 lines 47 – 55).

Claim 21 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the data is a message (column 5 lines 47 – 55).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
08/19/05

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100